



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/776,719	02/11/2004	Eric Henry Grosse	7	2822

7590 10/02/2007  
Docket Administrator (Room 3J-219)  
Lucent Technologies Inc.  
101 Crawfords Corner Road  
Holmdel, NJ 07733-3030

EXAMINER
----------

KAPLAN, BENJAMIN A

ART UNIT	PAPER NUMBER
----------	--------------

2139

MAIL DATE	DELIVERY MODE
-----------	---------------

10/02/2007

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

## Office Action Summary

Application No.

10/776,719

Applicant(s)

GROSSE, ERIC HENRY

Examiner

Benjamin A. Kaplan

Art Unit

2139

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 10 September 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1,3-12,15,16,18-27 and 30 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1,3-12,15,16,18-27 and 30 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 11 February 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- ☐ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☐ Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- ☐ Notice of Informal Patent Application
- ☐ Other: \_\_\_\_\_

**DETAILED ACTION**

1. Claims 1, 3-12, 15, 16, 18-27 & 30 are rejected.
2. Claims 2, 13, 14, 17, 28 & 29 are canceled.

***Claim Rejections - 35 USC § 103***

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 1, 7, 16 & 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Brustoloni, (US Patent Publication No.: US 2003/0236999 A1), in view of Maximum Security, Fourth Edition (Security).

**As per Claim 1:** Brustoloni teaches:

**- A method performed by a network edge router located at an incoming edge of an IP network, the method for authenticating indicated IP source addresses comprised in IP data packets to be transmitted through the IP network, the method comprising the steps of:**

(Brustoloni, Abstract, lines 1-11 " Ingress filtering has been adopted by the IETF as a methodology for preventing denial of service congestive attacks that spoof the source address in packets that are addressed to host server victims. Unless universally

adopted by all ISPs on the Internet, however, a packet's source address cannot be totally trusted to be its actual source address. To take advantage of benefits of ingress filtering as it is gradually deployed by ISPs around the Internet, differentiated classes of service are used to transport packets whose source address can be trusted and packets whose source address cannot be trusted.").

**- receiving an IP data packet at an incoming edge of an IP network, the IP data packet comprising an indicated IP source address**

(Brustoloni, Abstract, lines 11-12 "A packet received by an access or edge router").

**- determining whether said IP data packet having been received at said incoming edge of the IP network is consistent with it having originated at said indicated IP source address**

(Brustoloni, Paragraph 0008 lines 10-12 "With ingress filtering, ISP ingress routers will drop a packet that arrives in a port if the packet's source address does not match a prefix associated with the port.").

**- ensuring that a predetermined data field of said IP data packet contains a value representative of whether said IP data packet having been received at said incoming edge of the IP network is consistent with it having originated at said indicated IP source address.**

(Brustoloni, Paragraph 0012 lines 5-7 "If it is not properly associated, the packet is dropped. Otherwise, the packet is marked for forwarding in the privileged class of service.").

(Brustoloni, Paragraph 0014 lines 13-16 "Thus, if a packet obeys the desired predicate, it is transported in the privileged class of service, and if it does not, the packet is either dropped or segregated for transmission in the unprivileged class.").

In a system that is set up to mark a packet it is inherently necessary for it to have a field defined in which it is to do so.

Brustoloni does not explicitly teach the following limitation:

**- performing a Reverse Path Forwarding test on said IP data packet.**

However Security in analogous art teaches the above limitation.

(Security excerpt, page 2 paragraph 3 lines 1-2 "Cisco released the Unicast RPF (Reverse Path Forwarding) feature in IOS 12.0 (it was also in an earlier 11.1(CC) release) to try to mitigate problems caused by bad source addresses in packets.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of Security in to the teachings of Brustoloni, because one of ordinary skill in the art would be motivated to implement a system that is able to verify that packets being received already have a source address existing in your routers routing table to better protect your system, your clients or customers their of and other attached systems.

**As per Claim 7:** The rejection of claim 1 is incorporated and further Brustoloni teaches:

**- determining whether said IP data packet having been received at said incoming edge of the IP network has been received from a peer carrier which has already determined whether said IP data packet having been received at said incoming edge of the IP network is consistent with it having originated at said indicated IP source address**

(Paragraph 0022 lines 8-10 "At step 302, a determination is made whether that packet has arrived from an ISP that does supports ingress filtering.").

**- ensuring that the predetermined data field of said IP data packet contains a value representative of whether said IP data packet having been received at said incoming edge of the IP network was determined by said peer carrier to be consistent with it having originated at said indicated IP source address.**

(Paragraph 0022 lines 10-13 " If that source ISP does not support ingress filtering, then, at step 303, that packet is marked for transmission to its destination in an unprivileged class of service and is forwarded.").

(Paragraph 0022 lines 17-21 "If, however, at step 302, it is determined that the arriving packet came from an ISP that does support ingress filtering, such as ISP 101, then, at step 304, that packet is forwarded to its destination ISP in the same class in which it is already marked.").

(Paragraph 0014 lines 13-16 as seen in the rejection of claim 1).

Since Brustoloni's method either excepts the value marked by the prior router or places it own, the containing of a value in the predetermined data field is insured. The source ISP is the peer carrier.

**As per Claim 16:** Brustoloni teaches:

- **A network edge router located at an incoming edge of an IP network**

(Abstract, lines 11-12 "A packet received by an access or edge router").

- **the router adapted to authenticate indicated IP source addresses comprised in IP data packets to be transmitted through the IP network, the router comprising**

(Paragraph 0008 lines 10-12 as seen in the rejection of claim 1).

- **an input port which receives an IP data packet at the incoming edge of the IP network**

A router inherently has an input port which allows it to function.

- **the IP data packet comprising an indicated IP source address**

(Abstract, lines 1-11 as seen in the rejection of claim 1).

- **means for determining whether said IP data packet having been received at said**

**incoming edge of the IP network is consistent with it having originated at said indicated IP source address**

(Paragraph 0008 lines 10-12 as seen in the rejection of claim 1).

Packet's source address is checked for matching a prefix associated with the port inherently including means for determining whether said IP data packet having been received at said incoming edge of the IP network is consistent with it having originated at said indicated IP source address.

**- means for ensuring that a predetermined data field of said IP data packet contains a value representative of whether said IP data packet having been received at said incoming edge of the IP network is consistent with it having originated at said indicated IP source address.**

(Paragraph 0012 lines 5-7 as seen in the rejection of claim 1).

(Paragraph 0014 lines 13-16 as seen in the rejection of claim 1).

In a system that is set up to mark a packet it is inherently necessary for it to have a field defined in which it is to do so. Marking a packet based on a determination inherently includes a means for ensuring a value representative of that determination in the predetermined data field.

Brustoloni does not explicitly teach the following limitation:

**- means for performing a Reverse Path Forwarding test on said IP data packet.**

However Security in analogous art teaches the above limitation.



(Security excerpt, page 2 paragraph 3 lines 1-2 "Cisco released the Unicast RPF (Reverse Path Forwarding) feature in IOS 12.0 (it was also in an earlier 11.1(CC) release) to try to mitigate problems caused by bad source addresses in packets.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of Security in to the teachings of Brustoloni, because one of ordinary skill in the art would be motivated to implement a system that is able to verify that packets being received already have a source address existing in your routers routing table to better protect your system, your clients or customers their of and other attached systems.

A system with Reverse Path Forwarding implemented inherently has a means for its use.

**As per Claim 22:** The rejection of claim 16 is incorporated and further Brustoloni teaches:

**- means for determining whether said IP data packet having been received at said incoming edge of the IP network has been received from a peer carrier which has already determined whether said IP data packet having been received at said incoming edge of the IP network is consistent with it having originated at said indicated IP source address**

(Paragraph 0022 lines 8-10 as seen in the rejection of claim 7).

Determining if a packet has arrived from an ISP supporting filtering inherently includes a means for determining if the packet arrived from a peer carrier that has already made a determination.

**- means for ensuring that the predetermined data field of said IP data packet contains a value representative of whether said IP data packet having been received at said incoming edge of the IP network was determined by said peer carrier to be consistent with it having originated at said indicated IP source address.**

(Paragraph 0022 lines 10-13 as seen in the rejection of claim 7).

(Paragraph 0022 lines 17-21 as seen in the rejection of claim 7).

(Paragraph 0014 lines 13-16 as seen in the rejection of claim 1).

Since Brustoloni's method either excepts the value marked by the prior router or places it own, the containing of a value in the predetermined data field is insured.

The marking or acceptance of prior marking inherently include a means for ensuring a content of the predetermined data filed.

5. Claims 3 & 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Brustoloni, (US Patent Publication No.: US 2003/0236999 A1) and Security, in view of Building Internet Firewalls, 2nd Edition (O'Reilly).

**As per Claim 3:** Brustoloni and Security do not explicitly teach:

- said predetermined data field of said IP data packet comprises an otherwise unused data field of said IP data packet.

However O'Reilly in analogous art teaches the above limitation.

(O'Reilly excerpt page 3 section 4.1.1.2 IP layer lines 10-12 "The IP options field

Almost always empty; where options like the IP source route and the IP security options would be specified if they were used for a given packet").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of O'Reilly in to the teachings of Brustoloni and Security, because one of ordinary skill in the art would be motivated to make use of a field not otherwise in use in order to have a defined area of data space available for placing information to fully implement a control/security mechanism without interfering with the resources necessary for the rest of an environment to function.

**As per Claim 18:** The rejection of claim 16 is incorporated and further:

Claim 25 is the same as claim 3 and rejected under the same reasons as set forth in the rejection of claim 3.

6. Claims 4-6 & 19-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Brustoloni, (US Patent Publication No.: US 2003/0236999 A1) and Security, in view of IP Routing Protocols (IP Routing).

**As per Claim 4:** Brustoloni and Security do not explicitly teach:

**- said predetermined data field of said IP data packet comprises a Type of Service data field.**

However IP Routing in analogous art teaches the above limitation.

(IP Routing excerpt page 1 second to last paragraph "The type of service (TOS) field can be used to identify several quality of service (QOS) functions provided for an Internet application. Transit delay, throughput, precedence, and reliability can be requested with this field.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of IP Routing in to the teachings of Brustoloni and Security because one of ordinary skill in the art would be motivated to include a field capable of setting priority (delay, throughput, precedence). To ensure that packets marked for the privileged class of service (as in Brustoloni's method) will receive attention first.

**As per Claim 5:** Brustoloni teaches:

**- if said IP data packet having been received at said incoming edge of the IP network is not consistent with it having originated at said indicated IP source**

**address**

(Paragraph 0022 lines 10-13 as seen in the rejection of claim 7).

(Paragraph 0014 lines 13-16 as seen in the rejection of claim 1).

(Paragraph 0008 lines 10-12 as seen in the rejection of claim 1).

**- if said IP data packet having been received at said incoming edge of the IP network is consistent with it having originated at said indicated IP source address.**

(Paragraph 0012 lines 5-7 as seen in the rejection of claim 1).

(Paragraph 0022 lines 17-21 as seen in the rejection of claim 7).

Brustoloni and Security do not explicitly teach:

**- ensuring that the Type of Service data field contains a zero value**

However IP Routing in analogous art teaches the above and following limitation.

(IP Routing excerpt page 2 first 2 lines "Bit 3 is the delay bit (D bit). When set to 1 this TOS requests a short delay through an internet. Bit 3 is the delay bit (D bit). When set to 1 this TOS requests a short delay through an internet").

If setting Bit 3 to a 1 request a low delay then setting it to a 0 (the only other available position for a bit) obviously will result in a higher delay.

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of IP Routing in to the teachings of Brustoloni and Security, and enter a zero for the delay bit for failing to meet the desired

predicate, because one of ordinary skill in the art would be motivated to make sure that a packet failing a test of its source address and being marked for the unprivileged class of service would receive less priority than packets that pass the test.

**- ensuring that the Type of Service data field contains a non-zero value**

(IP Routing excerpt page 2 first 2 lines "Bit 3 is the delay bit (D bit). When set to 1 this TOS requests a short delay through an internet. Bit 3 is the delay bit (D bit). When set to 1 this TOS requests a short delay through an internet").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of IP Routing in to the teachings of Brustoloni and Security, and enter a one for the delay bit for successfully meeting the desired predicate, because one of ordinary skill in the art would be motivated to make sure that a packet passing a test of its source address and being marked for the privileged class of service would receive more priority than packets that failed the test.

**As per Claim 6:** Brustoloni teaches:

**- determining if the [specified] field already has a [specified affirming] value, and modifying the [specified] field to have a [specified affirming] value only if it does not already have a [specified affirming] value.**

(Paragraph 0022 lines 17-21 as seen in the rejection of claim 7).

(Paragraph 0012 lines 5-7 as seen in the rejection of claim 7).

If the mark (made by the preceding ISP in the packets path) is accepted then is the mark is not modified.

Brustoloni and Security do not explicitly teach:

**- the [specified] field as a Type of Service field**

However IP Routing in analogous art teaches the above and following limitation.

(IP Routing excerpt page 1 second to last paragraph as seen in the rejection of claim 4).

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of IP Routing in to the teachings of Brustoloni and Security because one of ordinary skill in the art would be motivated to include a field capable of setting priority (delay, throughput, precedence). To ensure that packets marked for the privileged class of service (as in Brustoloni's method) will receive attention first.

**- the [specified affirming] value as a non-zero value**

(IP Routing excerpt page 2 first 2 lines as seen in the rejection of claim 5).

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of IP Routing in to the teachings of Brustoloni and Security, and have or enter a one for the delay bit for successfully meeting the desired predicate, because one of ordinary skill in the art would be motivated to make sure that a packet passing a test of it's source address and being

Art Unit: 2139

marked for the privileged class of service would receive more priority than packets that failed the test.

**As per Claim 19:** Claim 19 is the same as claim 4 and rejected under the same reasons as set forth in the rejection of claim 4.

**As per Claim 20:** Claim 20 is the same as claim 5 and rejected under the same reasons as set forth in the rejection of claim 5.

Setting the delay bit to zero inherently includes a means for ensuring a zero value in the Type of Service field.

Setting the delay bit to one inherently includes a means for ensuring a non-zero value in the Type of Service field.

**As per Claim 21:** Claim 21 is the same as claim 6 and rejected under the same reasons as set forth in the rejection of claim 6.

Taking actions based on a fields contents inherently includes a means for determining a fields contents.

Setting the delay bit to one inherently includes a means for entering a non-zero value in the Type of Service field.



Art Unit: 2139

7. Claims 8, 9, 15, 23, 24 & 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Brustoloni, (US Patent Publication No.: US 2003/0236999 A1), in view of Access Control Lists: Overview and Guidelines (Cisco ACL)

**As per Claim 8:** Brustoloni teaches:

**- A method of processing IP data packets received from an IP network, the IP data packets comprising indicated IP source addresses and one or more of the IP data packets having been marked with indicia of whether the indicated IP source address comprised therein has been authenticated by the IP network, the method comprising the steps of:**

(Abstract, lines 1-11 as seen in the rejection of claim 1).

(Abstract, last line "class of service in which it is already marked.").

**- determining whether the indicated IP source address comprised in each one of said one or more of the IP data packets has been authenticated by the IP network**

(Paragraph 0022 lines 8-10 as seen in the rejection of claim 7).

A packet arriving from an ISP supporting filtering has been authenticated, a packet arriving from an ISP not supporting filtering has not been authenticated. The filtering is the authentication.

**- processing each one of the one or more of the IP data packets based on whether the indicated IP source address comprised therein has been authenticated by the IP network.**

(Paragraph 0022 lines 10-13 as seen in the rejection of claim 7).

(Paragraph 0022 lines 17-21 as seen in the rejection of claim 7).

The forwarding based on the class it decided to mark it as is the processing.

**- discarding each of said one or more IP data packets for which the indicated IP source address comprised therein has not been authenticated by the IP network.**

(Paragraph 0008 lines 10-12 as seen in the rejection of claim 1).

(Paragraph 0014 lines 13-16 as seen in the rejection of claim 1).

(Paragraph 0022 lines 10-13 as seen in the rejection of claim 7).

Dropping a packet inherently includes discarding the packet as claimed.

Brustoloni does not explicitly teach the following limitation:

**- performing a look up of one or more indicated IP source addresses comprised in one or more corresponding IP data packets which have been authenticated by the IP network, and wherein the step of processing each one of the one or more of the IP data packets based on whether the indicated IP source address comprised therein has been authenticated by the IP network further comprises discarding one or more of said IP data packets for which the indicated IP source address comprised therein has been authenticated by the IP network based on**

**said look up of said one or more indicated IP source addresses comprised in one or more corresponding IP data packets which have been authenticated by the IP network.**

However Cisco ACL in analogous art teaches the above limitation:

(Cisco ACL page 2 section What Access Lists Do paragraph 1 line 2-3 "Your router examines each packet to determine whether to forward or drop the packet, based on the criteria you specified within the access lists.").

(Cisco ACL page 2 section What Access Lists Do paragraph 2 line 1 "Access list criteria could be the source address of the traffic").

(Cisco ACL page 2 section Why You Should Configure Access Lists paragraph 3 "access lists can allow one host to access a part of your network, and prevent another host from accessing the same area. In Figure 6, Host A is allowed to access the Human Resources network and Host B is prevented from accessing the Human Resources network.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of Cisco ACL in to the teachings of Brustoloni, because one of ordinary skill in the art would be motivated to make use of a control list since, just because a packet isn't part of a DoS attack or using a spoofed source address that doesn't necessarily mean the sender of the packet has a right to access a destination or target resource.

**As per Claim 9:** The rejection of claim 8 is incorporated and further Brustoloni teaches:

**- said indicia of whether the indicated IP source address comprised in said one or more of the IP data packets has been authenticated by the IP network comprises a value contained in a predetermined data field of each of said IP data packets.**

(Paragraph 0012 lines 5-7 as seen in the rejection of claim 1).

(Paragraph 0014 lines 13-16 as seen in the rejection of claim 1).

In a system that is set up to mark a packet it is inherently necessary for it to have a field defined in which it is to do so.

**As per Claim 15:** The rejection of claim 8 is incorporated and further Brustoloni teaches:

**- prioritizing the one or more of the IP data packets based on whether the indicated IP source address comprised therein has been authenticated by the IP network, said IP data packets for which the indicated IP source address comprised therein has been authenticated by the IP network having a higher priority than said IP data packets for which the indicated IP source address comprised therein has not been authenticated by the IP network.**

(Paragraph 0022 lines 10-13 as seen in the rejection of claim 7).

(Paragraph 0014 lines 13-16 as seen in the rejection of claim 1).

(Paragraph 0012 lines 5-7 as seen in the rejection of claim 1).

Art Unit: 2139

Marking for class of service is prioritizing. The privileged class of service is the higher priority the unprivileged class of service is the lower priority.

**As per Claim 23:** Brustoloni teaches:

**- A server adapted to process IP data packets received from an IP network, the IP data packets comprising indicated IP source addresses and one or more of the IP data packets having been marked with indicia of whether the indicated IP source address comprised therein has been authenticated by the IP network, the server comprising:**

(Abstract, lines 11-12 "A packet received by an access or edge router").

A router in Brustoloni's method is this server.

**- means for determining whether the indicated IP source address comprised in each one of said one or more of the IP data packets has been authenticated by the IP network**

(Paragraph 0022 lines 8-10 as seen in the rejection of claim 7).

A packet arriving from an ISP supporting filtering has been authenticated, a packet arriving from an ISP not supporting filtering has not been authenticated. The filtering is the authentication.

This determination inherently contains a means for determining whether or not a packet has been authenticated.

**- means for processing each one of the one or more of the IP data packets based on whether the indicated IP source address comprised therein has been authenticated by the IP network.**

(Paragraph 0022 lines 10-13 as seen in the rejection of claim 7).

(Paragraph 0022 lines 17-21 as seen in the rejection of claim 7).

The forwarding based on the class it is marked inherently contains a means for processing a packet based on whether or not its source address has been verified.

**- means for discarding each of said one or more IP data packets for which the indicated IP source address comprised therein has not been authenticated by the IP network.**

(Paragraph 0008 lines 10-12 as seen in the rejection of claim 1).

(Paragraph 0022 lines 10-13 as seen in the rejection of claim 7).

(Paragraph 0014 lines 13-16 as seen in the rejection of claim 1).

Dropping a packet inherently includes a means for discarding it.

Brustoloni does not explicitly teach the following limitation:

**- means for performing a look up of one or more indicated IP source addresses comprised in one or more corresponding IP data packets which have been authenticated by the IP network, and wherein the means for processing each one of the one or more of the IP data packets based on whether the indicated IP**

**source address comprised therein has been authenticated by the IP network further comprises means for discarding one or more of said IP data packets for which the indicated IP source address comprised therein has been authenticated by the IP network based on said look up of said one or more indicated IP source addresses comprised in one or more corresponding IP data packets which have been authenticated by the IP network.**

However Cisco ACL in analogous art teaches the above limitation:

(Cisco ACL page 2 section What Access Lists Do paragraph 1 line 2-3 "Your router examines each packet to determine whether to forward or drop the packet, based on the criteria you specified within the access lists.").

(Cisco ACL page 2 section What Access Lists Do paragraph 2 line 1 "Access list criteria could be the source address of the traffic").

(Cisco ACL page 2 section Why You Should Configure Access Lists paragraph 3 "access lists can allow one host to access a part of your network, and prevent another host from accessing the same area. In Figure 6, Host A is allowed to access the Human Resources network and Host B is prevented from accessing the Human Resources network.").

An implemented Access Control List inherently has a means for performing its own functions.

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of Cisco ACL in to the teachings of Brustoloni, because one of ordinary skill in the art would be motivated to make use of a

Art Unit: 2139

control list since, just because a packet isn't part of a DoS attack or using a spoofed source address that doesn't necessarily mean the sender of the packet has a right to access a destination or target resource.

**As per Claim 24:** The rejection of claim 23 is incorporated and further Brustoloni teaches:

**- said indicia of whether the indicated IP source address comprised in said one or more of the IP data packets has been authenticated by the IP network comprises a value contained in a predetermined data field of each of said IP data packets.**

(Paragraph 0012 lines 5-7 as seen in the rejection of claim 1).

(Paragraph 0014 lines 13-16 as seen in the rejection of claim 1).

In a system that is set up to mark a packet it is inherently necessary for it to have a field defined in which it is to do so.

**As per Claim 30:** The rejection of claim 23 is incorporated and further Brustoloni teaches:

**- means for prioritizing the one or more of the IP data packets based on whether the indicated IP source address comprised therein has been authenticated by the IP network, said IP data packets for which the indicated IP source address comprised therein has been authenticated by the IP network having a higher**



**priority than said IP data packets for which the indicated IP source address comprised therein has not been authenticated by the IP network.**

(Paragraph 0022 lines 10-13 as seen in the rejection of claim 7).

(Paragraph 0014 lines 13-16 as seen in the rejection of claim 1).

(Paragraph 0012 lines 5-7 as seen in the rejection of claim 1).

Marking for class of service is prioritizing. The privileged class of service is the higher priority the unprivileged class of service is the lower priority.

The marking for class of service inherently includes a means for prioritizing data packets.

8. Claims 10 & 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Brustoloni, (US Patent Publication No.: US 2003/0236999 A1) and Cisco ACL, in view of Building Internet Firewalls, 2nd Edition (O'Reilly).

**As per Claim 10:** Brustoloni and Cisco ACL do not explicitly teach:

**- said predetermined data field of said IP data packet comprises an otherwise unused data field of said IP data packet.**

However O'Reilly in analogous art teaches the above limitation.

(O'Reilly excerpt page 3 section 4.1.1.2 IP layer lines 10-12 "The IP options field

Art Unit: 2139

Almost always empty; where options like the IP source route and the IP security options would be specified if they were used for a given packet”).

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of O'Reilly in to the teachings of Brustoloni and Security, because one of ordinary skill in the art would be motivated to make use of a field not otherwise in use in order to have a defined area of data space available for placing information to fully implement a control/security mechanism without interfering with the resources necessary for the rest of an environment to function.

**As per Claim 25:** The rejection of claim 24 is incorporated and further:

Claim 25 is the same as claim 10 and rejected under the same reasons as set forth in the rejection of claim 10.

9. Claims 11, 12, 26 & 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Brustoloni, (US Patent Publication No.: US 2003/0236999 A1) and Cisco ACL, in view of IP Routing Protocols (IP Routing).

**As per Claim 11:** The limitation of Claim 11 is a restatement of the limitation of claim 4 and is rejected under similar reasoning as set forth in the rejection of claim 4.

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of IP Routing in to the teachings of Brustoloni and Cisco ACL because one of ordinary skill in the art would be motivated to

include a field capable of setting priority (delay, throughput, precedence). To ensure that packets marked for the privileged class of service (as in Brustoloni's method) will receive attention first.

**As per Claim 12:** The limitations of Claim 12 are a restatement of the limitation of claim 5 and are rejected under similar reasoning as set forth in the rejection of claim 5.

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of IP Routing in to the teachings of Brustoloni and Cisco ACL and enter a zero for the delay bit for failing to meet the desired predicate, because one of ordinary skill in the art would be motivated to make sure that a packet failing a test of it's source address and being marked for the unprivileged class of service would receive less priority than packets that pass the test.

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of IP Routing in to the teachings of Brustoloni and Cisco ACL and enter a one for the delay bit for successfully meeting the desired predicate, because one of ordinary skill in the art would be motivated to make sure that a packet passing a test of it's source address and being marked for the privileged class of service would receive more priority than packets that failed the test.

**As per Claim 26:** The limitation of Claim 26 is a restatement of the limitation of claim 11 and is rejected under similar reasoning as set forth in the rejection of claim 11.

**As per Claim 27:** Claim 27 is a restatement of the limitation of claim 12 and is rejected under similar reasoning as set forth in the rejection of claim 12.

***Response to Amendment and Affidavit***

10. This Affidavit filed on 9/10/07 was filed under 37 CFR 1.132, which is treated as 37 CFR 1.131 because applicant attempts to establish the rejected claims prior to the effective date of the Brustolini reference under 35 USC 102(a). Rejection in Office action 6/7/07.

The Affidavit is unexecuted because it was declared by a disqualified party. See MPEP, 37 CFR 1.131, 1.42, 1.43, 1.47. The Affidavit also fails to establish reduction to practice prior to the effective date of the reference, or conception of the invention prior to the effective date of the reference coupled with due diligence from prior to said date to a subsequent reduction to practice or to the filing of the application. The exhibit A appears to show the conception of the invention (June 03). However, applicant fails to establish due diligence from June 03 to the filing of the application, February 04.

Thus, the Affidavit filed on 9/10/07 is treated under 37 CFR 1.131 has been considered but is ineffective to overcome the Brustolini reference.

11. As the Affidavit is presently ineffective the Brustolini reference remains available under 35 USC 102(a) and cannot be excluded under 35 USC 103(c) at this time.

***Conclusion***

12. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin A. Kaplan whose telephone number is 571-270-3170. The examiner can normally be reached on 7:30 a.m. - 5:00 p.m. E.S.T.:

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2139

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Benjamin Kaplan

  
SYED A. ZIA  
PRIMARY EXAMINER